ICUFOR
Cursos de Formación Permanente Universitaria

Curso de Formación Permanente

Ciberseguridad en los Proyectos de Transformación Digital de la Administración Pública

6 ECTS | 150 horas | Online, a tu ritmo

Formación acreditada por
Universidad de Vitoria-Gasteiz EUNEIZ



Acerca de ICUFOR

ICUFOR es un centro privado de formación online, Centro Acreditado y Autorizado por la Universidad EUNEIZ de Vitoria-Gasteiz. Diseñamos e impartimos Cursos de Formación Permanente universitarios, pensados para la actualización y la especialización de profesionales en activo.

Nuestros cursos se estudian a tu ritmo en un campus virtual propio y terminan con el diploma de la Universidad EUNEIZ y con certificados de ICUFOR verificables.

Centro acreditado
Universidad EUNEIZ

100 % online
Campus virtual propio

Equipo docente
Disponible todo el curso



Metodología de estudio

Campus virtual propio
Estudias desde cualquier lugar y dispositivo, sin horarios.

Aprendizaje autónomo, pero acompañado
Tú marcas el ritmo y nuestro equipo de docentes resuelve tus dudas y orienta tu estudio.

Contenido del curso en PDF
El material principal, para estudiarlo a fondo, tema a tema.

Abstract de cada tema
Su síntesis, para situarte al empezar y repasar al final.

Presentación con los aspectos clave
Lo esencial de cada bloque, para jerarquizar y fijar.

Cuestionarios de evaluación
De respuesta múltiple, uno por tema.



Campus virtual

Mis cursos
Tu progreso y el siguiente tema por estudiar

Materiales
Contenido en PDF, Abstract y presentación con los aspectos clave

Cuestionarios de evaluación
Tu nota y la revisión de tus respuestas

Equipo docente
Consulta por escrito, chat y asesor de IA a cualquier hora

Secretaría
Certificados en PDF con código de verificación

Pagos y facturas
Descarga de facturas en PDF



Presentación del programa



Amplía tu formación con el Curso de Formación Permanente en Ciberseguridad en los Proyectos de Transformación Digital de la Administración Pública de ICUFOR, diseñado para profesionales que deseen especializarse en la protección de sistemas y servicios digitales del sector público. En un contexto donde las amenazas cibernéticas evolucionan constantemente, las instituciones públicas requieren expertos capaces de implementar estrategias de seguridad robustas que garanticen la confianza ciudadana y la continuidad de los servicios esenciales.

Duración
150 horas

Créditos
6 Créditos ECTS

Metodología
Online

Matriculación
Permanente

Objetivos del curso

Comprender los fundamentos de la transformación digital en la Administración Pública, identificando su vinculación estructural con la ciberseguridad y el ecosistema institucional que la sustenta.

Conocer el marco normativo multinivel de la ciberseguridad pública, diferenciando la legislación europea, nacional y sectorial aplicable a la Administración.

Analizar la gobernanza de la ciberseguridad y los requisitos del Esquema Nacional de Seguridad, aplicando sus principios de categorización, protección y adecuación en las organizaciones públicas.

Aplicar metodologías de análisis y gestión de riesgos de ciberseguridad, utilizando marcos y herramientas de referencia como MAGERIT y PILAR en proyectos de transformación digital.

Identificar los requisitos de seguridad en infraestructuras tecnológicas, servicios en la nube y desarrollo de aplicaciones digitales, incorporando controles de protección adecuados en cada fase de su ciclo de vida.

Fundamentar la protección de datos personales y la privacidad en los proyectos tecnológicos públicos, relacionando las exigencias del RGPD con las medidas de ciberseguridad del ENS.

Desarrollar capacidades de gestión de incidentes y continuidad de servicios públicos digitales, implementando protocolos de detección, respuesta, recuperación y análisis forense.

Saber llevar a cabo procesos de contratación segura, auditoría y mejora continua de la ciberseguridad, aplicando criterios de cumplimiento y lecciones aprendidas de casos reales.

Temario

01 Fundamentos de la transformación digital en la Administración Pública y su vinculación con la ciberseguridad

1.1. Concepto, alcance y dimensiones de la transformación digital en el sector público
1.2. Evolución histórica de la modernización tecnológica en las Administraciones Públicas españolas y europeas
1.3. Principales proyectos y servicios de transformación digital en la Administración Pública actual
1.4. La ciberseguridad como requisito estructural de la transformación digital pública
1.5. Ecosistema institucional de ciberseguridad pública en España

Temario

02 Marco normativo y regulatorio de la ciberseguridad aplicable a la Administración Pública

2.1. Arquitectura jurídica multinivel de la ciberseguridad en el sector público
2.2. Normativa europea fundamental en materia de ciberseguridad
2.3. El Esquema Nacional de Seguridad: fundamento legal y estructura general
2.4. Legislación española complementaria en materia de seguridad de la información pública
2.5. Estrategias nacionales de ciberseguridad y su impacto operativo en la Administración
2.6. Normativa sectorial específica aplicable a ámbitos concretos de la Administración
2.7. Responsabilidades legales derivadas del incumplimiento normativo en ciberseguridad

Temario

03 Gobernanza de la ciberseguridad en las organizaciones públicas

3.1. Concepto y modelos de gobernanza de la ciberseguridad aplicados al sector público
3.2. Estructuras organizativas para la ciberseguridad en las entidades públicas
3.3. Política de seguridad de la información: diseño, aprobación y despliegue
3.4. Integración de la ciberseguridad en la planificación estratégica y en la gestión por proyectos
3.5. Cultura de ciberseguridad, formación y concienciación del personal público
3.6. Indicadores de gobernanza y cuadros de mando para la dirección de la ciberseguridad

Temario

04 El Esquema Nacional de Seguridad: principios, requisitos y medidas de protección

4.1. Principios básicos del Esquema Nacional de Seguridad y su aplicación práctica
4.2. Categorización de los sistemas de información en la Administración Pública
4.3. Marco organizativo de medidas de seguridad del ENS
4.4. Medidas de seguridad del marco operacional
4.5. Medidas de protección específicas del ENS
4.6. Perfiles de cumplimiento específicos y guías CCN-STIC como apoyo a la implementación
4.7. Proceso de adecuación, declaración de aplicabilidad y obtención de la conformidad
4.8. Interrelación del ENS con otros marcos normativos y estándares internacionales de seguridad

Temario

05 Análisis y gestión de riesgos de ciberseguridad en proyectos de transformación digital

5.1. Fundamentos conceptuales de la gestión de riesgos de ciberseguridad
5.2. Marcos y estándares de referencia para el análisis de riesgos
5.3. Identificación y valoración de activos en los sistemas de información públicos
5.4. Identificación de amenazas y vulnerabilidades en el contexto de la Administración Pública
5.5. Estimación del riesgo, determinación del nivel de riesgo aceptable y estrategias de tratamiento
5.6. Herramientas de soporte al análisis de riesgos: PILAR y su aplicación práctica
5.7. Integración del análisis de riesgos en la toma de decisiones del proyecto y comunicación a la dirección

Temario

06 Seguridad en las infraestructuras tecnológicas y los servicios en la nube de la Administración Pública

6.1. Arquitecturas tecnológicas habituales en los proyectos de transformación digital pública
6.2. Seguridad en redes y comunicaciones de la Administración Pública
6.3. Estrategia de adopción segura de servicios en la nube en el sector público
6.4. Requisitos de seguridad para los modelos de servicio IaaS, PaaS y SaaS
6.5. Gestión segura de identidades, accesos y privilegios en entornos tecnológicos complejos
6.6. Protección del puesto de trabajo digital y de los dispositivos móviles del empleado público
6.7. Monitorización continua y detección de amenazas en infraestructuras públicas

Temario

07 Protección de datos personales y privacidad en los proyectos de transformación digital pública

7.1. Marco jurídico de la protección de datos aplicable a la Administración Pública
7.2. Convergencia operativa entre protección de datos y ciberseguridad
7.3. Evaluaciones de impacto en protección de datos en proyectos tecnológicos públicos
7.4. Privacidad desde el diseño y por defecto en los servicios digitales públicos
7.5. Gestión de brechas de seguridad con afectación a datos personales
7.6. Retos de privacidad en las tecnologías emergentes aplicadas al sector público

Temario

08 Seguridad en el ciclo de vida del desarrollo de servicios y aplicaciones digitales para la Administración

8.1. Principios de desarrollo seguro de software aplicados al sector público
8.2. Integración de la seguridad en las metodologías de desarrollo ágil y DevSecOps
8.3. Requisitos de seguridad en las fases de análisis, diseño y arquitectura del servicio digital
8.4. Prácticas de codificación segura y prevención de vulnerabilidades
8.5. Verificación y pruebas de seguridad del software
8.6. Seguridad en interfaces de programación de aplicaciones y servicios de interoperabilidad
8.7. Gestión segura del despliegue, la configuración y el mantenimiento de las aplicaciones en producción

Temario

09 Gestión de incidentes de ciberseguridad y continuidad de los servicios públicos digitales

9.1. Marco conceptual y normativo de la gestión de incidentes de ciberseguridad en la Administración
9.2. Estructura y operación de los equipos de respuesta ante incidentes en el sector público
9.3. Proceso integral de gestión del incidente de ciberseguridad
9.4. Lecciones aprendidas y mejora del proceso de respuesta a incidentes
9.5. Planificación de la continuidad de los servicios públicos digitales
9.6. Realización de simulacros y ejercicios de ciberseguridad en la Administración

10 Contratación pública de servicios tecnológicos con requisitos de ciberseguridad

10.1. Marco jurídico de la contratación pública de servicios TIC y su relación con la ciberseguridad
10.2. Definición de requisitos de ciberseguridad en los pliegos de prescripciones técnicas
10.3. Evaluación de la capacidad y solvencia en ciberseguridad de los licitadores
10.4. Gestión de la seguridad en la cadena de suministro tecnológico de la Administración
10.5. Acuerdos de nivel de servicio con componentes de seguridad y mecanismos de penalización

Temario

11 Auditoría, cumplimiento y mejora continua de la ciberseguridad en la Administración Pública

11.1. La auditoría de ciberseguridad en el marco del Esquema Nacional de Seguridad
11.2. Estándares y marcos de referencia para la auditoría de seguridad de la información
11.3. Herramientas de evaluación y diagnóstico del nivel de seguridad
11.4. Gestión de las no conformidades y planes de acción correctiva
11.5. Sistemas de gestión de la seguridad de la información en el sector público
11.6. Métricas, indicadores clave de rendimiento y reporting de la postura de seguridad

12 Casos prácticos integradores y lecciones aprendidas en proyectos reales de transformación digital segura

12.1. Metodología de análisis de casos prácticos en ciberseguridad pública
12.2. Caso práctico de implantación del ENS y migración segura a la nube en una Administración Pública
12.3. Caso práctico de gestión de un incidente de ciberseguridad grave en una Administración autonómica
12.4. Síntesis de buenas prácticas y factores críticos de éxito en la ciberseguridad de los proyectos de transformación digital pública

Titulación y certificados

Diploma de la Universidad EUNEIZ

Al aprobar todos los cuestionarios de evaluación recibes el **diploma en formato digital** de Curso de Formación Permanente, con sus 6 créditos ECTS y 150 horas.

Certificados de ICUFOR

Se descargan en PDF desde la Secretaría del campus, con un código único y QR para verificarlos.



Universidad de Vitoria-Gasteiz EUNEIZ

Proceso de matriculación

1 **Pulsa «Matricularme» en la ficha del curso**
Completa tus datos personales y de facturación.

2 **Elige la forma de pago**
Tarjeta, PayPal o transferencia bancaria.

3 **Entra en el campus y empieza**
Recibes por correo tus datos de acceso y, en cuanto se confirma el pago, tienes el temario completo. La matrícula está abierta todo el año.

Matricúlate | Más información



Métodos de pago

Pago único
El precio se abona una sola vez, sin cuotas ni renovaciones.

Seguridad
Pago online en la pasarela de Stripe o de PayPal.

Flexibilidad
Tarjeta de crédito o débito, PayPal o transferencia.

Acceso inmediato
Con tarjeta o PayPal, el campus se activa al momento.

Simplicidad
Matrícula y pago en dos pasos.

Facturación
Facturas en «Pagos y facturas» del campus.



¿Por qué elegir ICUFOR?

01

Formación accesible

Formación universitaria rigurosa y acreditada, íntegramente online y compatible con tu trabajo.

02

Calidad universitaria

Cada curso está acreditado por la Universidad EUNEIZ, con su memoria académica y sus créditos ECTS.

03

Impulso a tu carrera

Contenidos de utilidad práctica y una titulación que suma en méritos, concursos y bolsas de empleo.

04

Especialización

Cada curso trata una única temática a fondo: combínalos y construye tu propio itinerario.

05

Atención de calidad

Consultas al equipo docente por escrito o por chat, y un asesor de IA a cualquier hora.

¿Por qué elegir ICUFOR?

06
Contenidos actualizados
Los cursos se revisan periódicamente para incorporar las novedades de cada ámbito.

07
El curso, por escrito
Cada tema en tres formatos: contenido en PDF, Abstract y presentación con los aspectos clave.

08
Autónomo, pero acompañado
Tú decides tu ritmo y nuestro equipo de docentes resuelve tus dudas y orienta tu estudio.

09
Enseñanza adaptada
Sin horarios ni conexiones obligatorias: seis meses para terminar, ampliables si lo necesitas.

10
Estudio sencillo e intuitivo
Un campus virtual propio, sin instalar nada y accesible desde cualquier dispositivo.

¿Necesitas más información?

Te contamos cómo funciona el curso, los plazos y la titulación, sin compromiso.

www.icufor.com

info@icufor.com

+34 858 895 080

+34 746 044 519

Formación acreditada por Universidad de Vitoria-Gasteiz EUNEIZ

